在安全防火墙威胁防御上配置远程访问VPN服务的威胁检测

目录

简介

本文档介绍在思科安全防火墙威胁防御(FTD)上为远程访问VPN服务配置威胁检测的流程。

先决条件

思科建议您了解以下主题：

- 思科安全防火墙威胁防御(FTD)。
- 思科安全防火墙管理中心(FMC)。
- FTD上的远程访问VPN (RAVPN)。

要求

以下列出的思科安全防火墙威胁防御版本支持这些威胁检测功能：

- 7.0.6.3中支持的7.0版本系列->

使用的组件

本文档中介绍的信息基于以下硬件和软件版本：

- 思科安全防火墙威胁防御虚拟版本7.0.6.3。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

远程访问VPN服务的威胁检测功能可供您防御以下任何场景：

1. 连接尝试使远程访问VPN服务无效。也就是说，尝试连接到仅供内部使用的服务。
2. 客户端启动攻击，攻击者从单个主机重复尝试连接到远程访问VPN头端，但发起攻击后仍未完成连接。
3. 对远程访问VPN服务重复尝试的身份验证失败（暴力用户名/密码扫描攻击）。

即使这些攻击尝试访问失败，它们也会消耗计算资源，并阻止有效用户连接到远程访问VPN服务。

当您启用这些服务时，安全防火墙会自动避开超过配置阈值的主机（IP地址），以阻止进一步尝试，直到您手动删除IP地址的回避。

注意：默认情况下会禁用远程访问VPN的所有威胁检测服务。

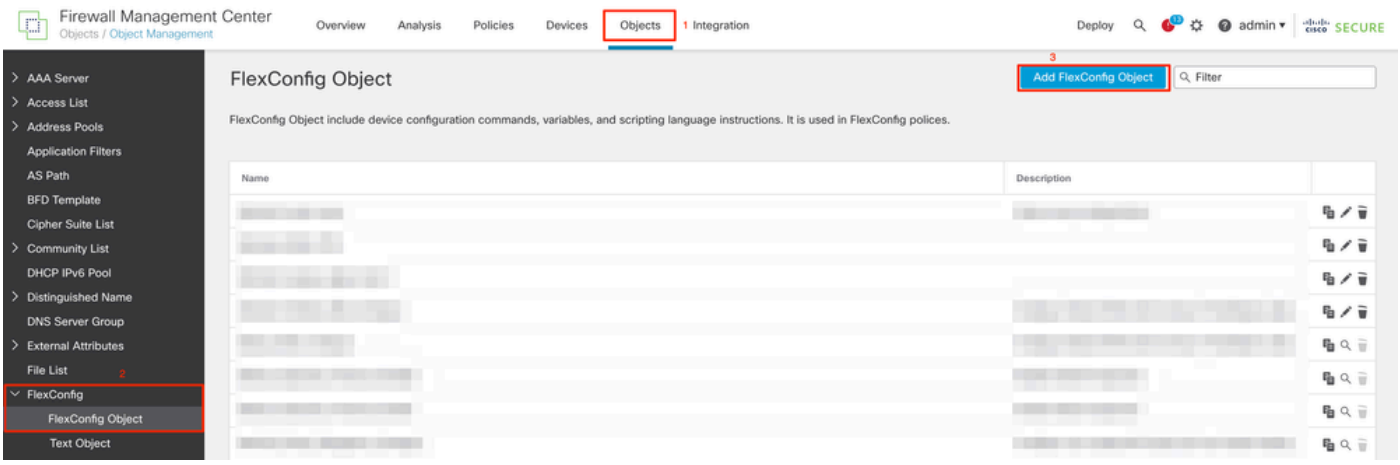
配置

注意：当前仅通过FlexConfig支持安全防火墙威胁防御上这些功能的配置。

---

1. 登录安全防火墙管理中心。

2. 要配置FlexConfig对象，请导航到对象>对象管理> FlexConfig > FlexConfig对象，然后单击添加FlexConfig对象。



3. 打开Add FlexConfig Object窗口后，添加所需的配置以启用远程访问VPN的威胁检测功能：

- FlexConfig对象名称：enable-threat-detection-ravpn
- FlexConfig对象说明：为远程访问VPN服务启用威胁检测。
- 部署：一次
- 类型：附加。
- 文本框：根据下文介绍的可用功能添加“threat detection service”命令。

注意：您可以使用同一FlexConfig对象为远程访问VPN启用3个可用的威胁检测功能，也可以为要启用的每个功能单独创建一个FlexConfig对象。

功能1：尝试连接到仅内部（无效）VPN服务的威胁检测

要启用此服务，请在FlexConfig object文本框中添加threat detection service invalid-vpn-access命令。

功能2：远程访问VPN客户端发起攻击的威胁检测

要启用此服务，请在FlexConfig object文本框中添加threat detection service remote-access-client-initiations hold-down <minutes> threshold <count>命令，其中：

- hold-down <minutes>定义最后一次启动尝试之后的一段时间，在此期间将计算连续的连接尝试。如果在此时间段内连续连接尝试次数达到配置的阈值，则会避开攻击者的IPv4地址。您可以将此时间段设置为1到1440分钟。
- threshold <count>是在抑制期间触发shun所需的连接尝试次数。可以将阈值设置为5到100。

例如，如果抑制期是10分钟，阈值是20，则如果在任何10分钟间隔内有20次连续的连接尝试，则会自动避开IPv4地址。

注意：在设置抑制和阈值时，请将NAT使用情况考虑在内。如果使用PAT（允许来自同一IP地址的许多请求），请考虑较高的值。这样可确保有效用户有足够的时间进行连接。例如，在酒店中，许多用户可能会尝试在短时间内建立连接。

功能3：远程访问VPN身份验证失败的威胁检测

要启用此服务，请在FlexConfig object文本框中添加threat detection service remote-access-authentication hold-down<minutes> threshold <count>命令，其中：

- hold-down <minutes>定义最后一次失败尝试之后统计连续失败的时间段。如果连续身份验证失败数在此期间达到配置的阈值，攻击者的IPv4地址将被回避。您可以将此时间段设置为1到1440分钟。
- threshold <count>是在抑制期间触发shun所需的失败身份验证尝试次数。您可以设置介于1和100之间的阈值。

例如，如果抑制期是10分钟，阈值是20，则如果在任何10分钟跨度内连续发生20次身份验证失败，则会自动回避IPv4地址。

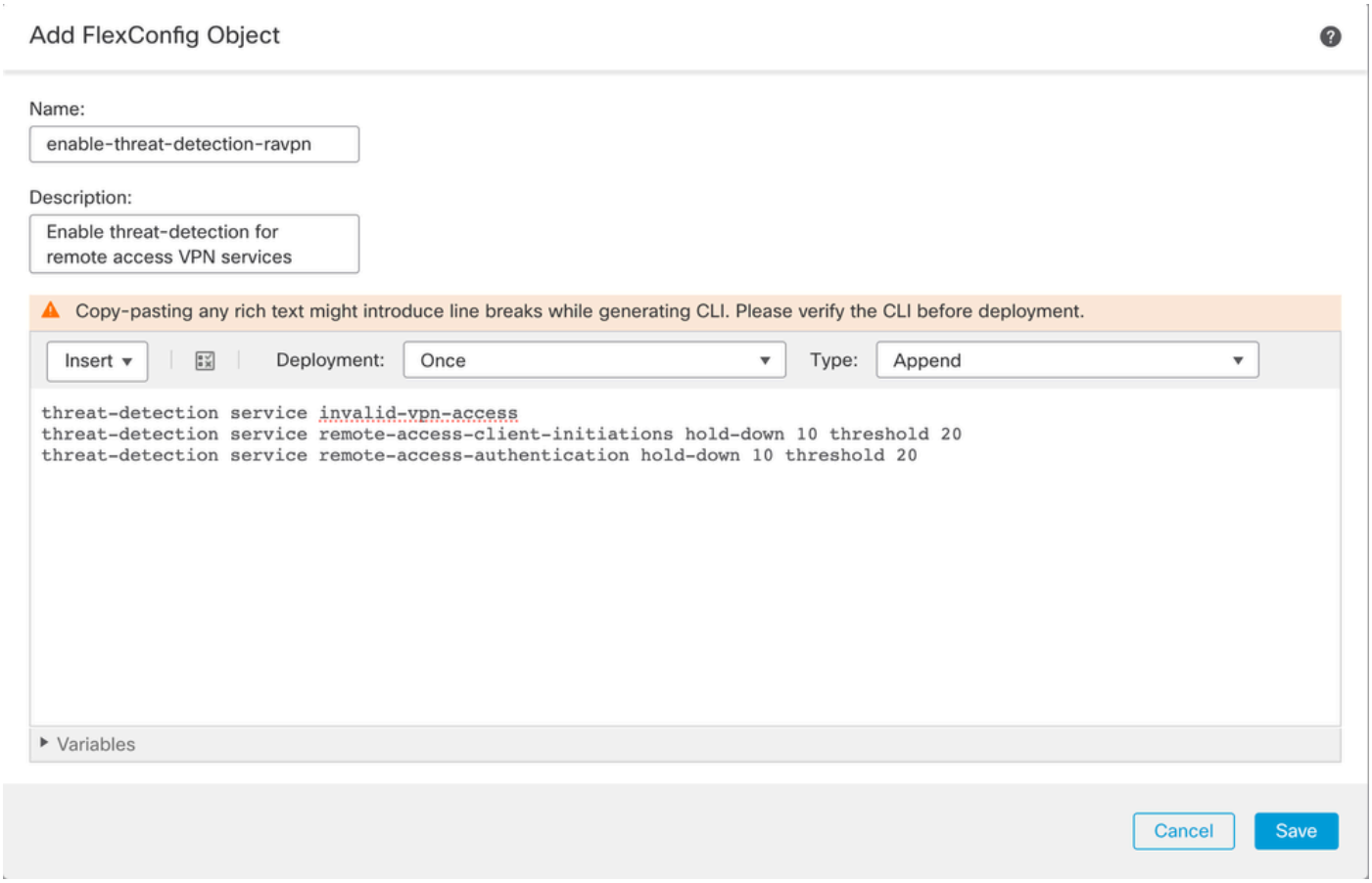
注意：在设置抑制和阈值时，请将NAT使用情况考虑在内。如果使用PAT（允许来自同一IP地址的许多请求），请考虑较高的值。这样可确保有效用户有足够的时间进行连接。例如，在酒店中，许多用户可能会尝试在短时间内建立连接。

注意：尚不支持通过SAML进行身份验证失败。

此示例配置启用远程访问VPN的三项可用威胁检测服务，抑制期为10分钟，阈值为20（客户端发起和身份验证尝试失败）。根据您的环境要求配置hold-down和threshold值。

此示例使用单个FlexConfig对象来启用3个可用功能。

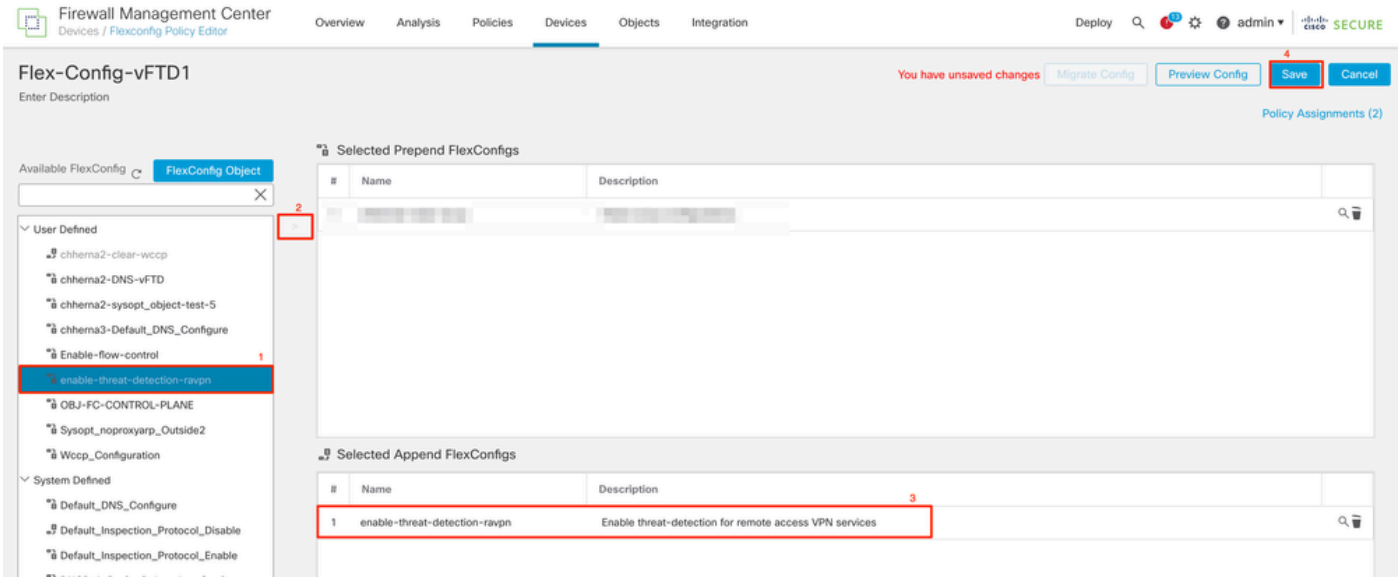
```
threat-detection service invalid-vpn-access
threat-detection service remote-access-client-initiations hold-down 10 threshold 20
threat-detection service remote-access-authentication hold-down 10 threshold 20
```



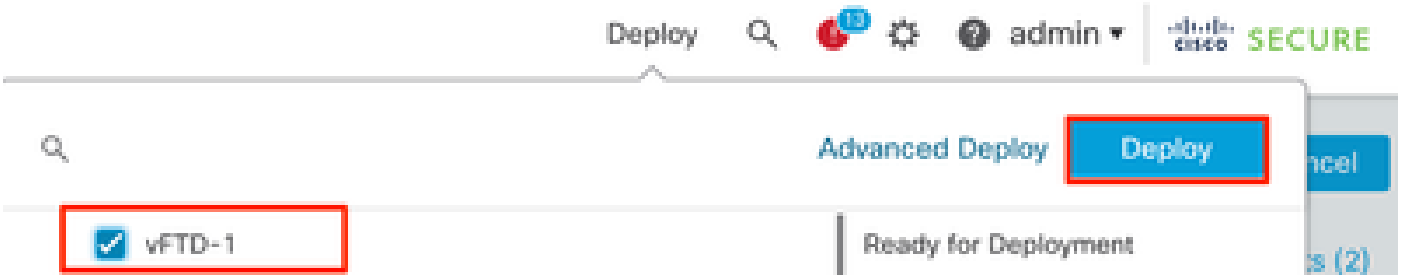
4. 保存FlexConfig对象。

5. 导航到设备> FlexConfig，然后选择分配给安全防火墙的FlexConfig策略。

6. 从左侧窗格中显示的可用FlexConfig对象中，选择在步骤3中配置的FlexConfig对象，单击“>”，然后保存更改。



7. 部署更改并验证。



验证

要显示威胁检测RAVPN服务的统计信息，请登录到FTD的CLI并运行show threat-detection service [service] [entries|details]命令。其中服务可以是：remote-access-authentication、remote-access-client-initiations或invalid-vpn-access。

您可以通过添加以下参数来进一步限制视图：

- entries -仅显示威胁检测服务所跟踪的条目。例如，身份验证尝试失败的IP地址。
- details -显示服务详细信息和服务条目。

运行show threat-detection 服务命令以显示所有已启用的威胁检测服务的统计信息。

<#root>

```
ciscoftd# show threat-detection service

Service: invalid-vpn-access State : Enabled

    Hold-down : 1 minutes
    Threshold : 1
```

```
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0

Service: remote-access-authentication State : Enabled

    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
    Total entries: 2

Name: remote-access-client-initiations State : Enabled

    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
```

要查看针对远程访问身份验证服务跟踪的潜在攻击者的更多详细信息，请运行show threat-detection service <service> entries命令。

```
ciscoftd# show threat-detection service remote-access-authentication entries
Service: remote-access-authentication
    Total entries: 2

Idx Source              Interface            Count          Age        Hold-down
--- ------------------- -------------------- -------------- ---------- ---------
  1 192.168.100.101/ 32              outside              1        721         0
  2 192.168.100.102/ 32              outside              2        486       114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

要查看特定威胁检测远程接入VPN服务的一般统计信息和详细信息，请运行show threat-detection service <service> details命令。

```
ciscoftd# show threat-detection service remote-access-authentication details
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
```

```
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
     Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1         721           0
  2 192.168.100.102/ 32              outside              2         486         114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

注意：条目仅显示威胁检测服务跟踪的IP地址。如果IP地址满足要规避的条件，则blocking 计数增加，且IP地址不再显示为条目。

此外，您可以监控VPN服务应用的分流器，并使用以下命令删除单个IP地址或所有IP地址的分流器：

- show shun [ip_address]

显示回避的主机，包括通过威胁检测自动回避的VPN服务或使用shun命令手动回避的主机。或者，可以将视图限制为指定的IP地址。

- no shun ip_address [interface if_name]

仅从指定的IP地址删除shun。或者，如果地址在多个接口上被避开并且您希望在某些接口上保持适当，则可以指定回避的接口名称。

- clear shun

从所有IP地址和所有接口删除shun。

注意：VPN服务的威胁检测规避的IP地址不会出现在show threat-detection shun命令中，该命令仅应用于扫描威胁检测。

要读取与远程访问VPN的威胁检测服务相关的每个命令输出的所有详细信息和可用Syslog消息，请参阅命令参考文档。

相关信息

- 如需其他帮助，请联系技术支持中心(TAC)。需要有效的支持合同：思科全球支持联系人。
- 您还可以访问Cisco VPN社区此处。
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。